

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Commissioner
 US Department of Commerce
 United States Patent and Trademark
 Office, PCT
 2011 South Clark Place Room
 CP2/5C24
 Arlington, VA 22202
 ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 01 March 2001 (01.03.01)	
International application No. PCT/US00/09800	Applicant's or agent's file reference GIC-574 PCT
International filing date (day/month/year) 12 April 2000 (12.04.00)	Priority date (day/month/year) 04 May 1999 (04.05.99)
Applicant SAFADI, Reem et al	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:

04 December 2000 (04.12.00)

☐ in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was
☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

<p>The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland</p> <p>Facsimile No.: (41-22) 740.14.35</p>	<p>Authorized officer</p> <p>Claudio Borton</p> <p>Telephone No.: (41-22) 338.83.38</p>
--	---

INTERNATIONAL COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

REC'D 07 AUG 2001

WIPO

PCT

14

Applicant's or agent's file reference GIC-574 PCT	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/US00/09800	International filing date (day/month/year) 12 APRIL 2000	Priority date (day/month/year) 04 MAY 1999
International Patent Classification (IPC) or national classification and IPC IPC(7): HO4L 9/00 and US Cl.: 380/258		
Applicant GENERAL INSTRUMENT CORPORATION		

- This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
- This **REPORT** consists of a total of 7 sheets.
☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority. (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).
 These annexes consist of a total of 4 sheets.
- This report contains indications relating to the following items:
 - ☒ Basis of the report
 - ☐ Priority
 - ☐ Non-establishment of report with regard to novelty, inventive step or industrial applicability
 - ☐ Lack of unity of invention
 - ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
 - ☐ Certain documents cited
 - ☐ Certain defects in the international application
 - ☐ Certain observations on the international application

Date of submission of the demand 04 DECEMBER 2000	Date of completion of this report 20 JUNE 2001
Name and mailing address of the IPEA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	Authorized officer TOD SWANN <i>James R. Matthews</i>
Facsimile No. (703) 305-3230	Telephone No. (703) 308-7791

I. Basis of the report**1. With regard to the elements of the international application:***

- ☐ the international application as originally filed
- ☒ the description:
pages: (See Attached) _____, as originally filed
pages: _____, filed with the demand
pages: _____, filed with the letter of _____
- ☒ the claims:
pages: (See Attached) _____, as originally filed
pages: _____, as amended (together with any statement) under Article 19
pages: _____, filed with the demand
pages: _____, filed with the letter of _____
- ☒ the drawings:
pages: (See Attached) _____, as originally filed
pages: _____, filed with the demand
pages: _____, filed with the letter of _____
- ☒ the sequence listing part of the description: (See Attached) _____, as originally filed
pages: _____, filed with the demand
pages: _____, filed with the letter of _____

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language _____ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 33.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international

- ☐ contained in the international application in printed form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☒ The amendments have resulted in the cancellation of:

- ☒ the description, pages: NONE
- ☒ the claims, Nos: NONE
- ☒ the drawings, sheet: 42 NONE

5. ☐ This report has been drawn as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

** Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).*

***Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/US00/09800

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**1. statement**

Novelty (N)	Claims	<u>8, 15, 17, 22-42</u>	YES
	Claims	<u>1-7, 9-14, 16, and 18-21</u>	NO
Inventive Step (IS)	Claims	<u>NONE</u>	YES
	Claims	<u>1-42</u>	NO
Industrial Applicability (IA)	Claims	<u>1-42</u>	YES
	Claims	<u>NONE</u>	NO

2. citations and explanations (Rule 70.7)

Claims 1-7, 9-14, 16, 18-21 lack novelty under PCT Article 33(2) as being anticipated by MacDoran.

Claim 1: MacDoran teaches pre-encrypting the content (col. 28, lines 61-67 and col. 29, lines 45-51), forwarding the pre-encrypted content to a server (col. 10, lines 26-54), providing a first tag to a user terminal, the first tag being associated with a second tag (col. 10, lines 31-54), the second tag acting as a reference to the pre-encrypted content and associated first tag, wherein the first and second tags are unique to the pre-encrypted content and are tracked by a pre-encryption controller (col. 10, lines 31-54), providing at least the second tag to the server (col. 10, lines 48-54), communicating the pre-encrypted content from the server to the user terminal via a first communication path (col. 10, lines 26-54), communicating an entitlement authorization associated with the pre-encrypted content to the user terminal via a second communication path independent of the first communication path (col. 10, lines 48-54), and determining whether the user terminal is authorized to access the pre-encrypted content based on the entitlement authorization and the first tag upon demand of the content by a user (col. 10, lines 50-63).

Claim 2: MacDoran teaches claim 1. MacDoran teaches the server is a main server (Fig. 1, #150), the main server communicates the pre-encrypted content and first tag to the user terminal via a local distribution server (Fig. 1, #110), and the pre-encryption controller is in communication with a local distribution controller communicates the entitlement authorization to the user terminal (Fig. 1, #109).

Claim 3: MacDoran teaches claim 2. MacDoran teaches the first tag is an opaque data block (ODB) (col. 10, lines 31-54) and the second tag is a unique reference handle (URH) (col. 10, lines 48-54).

Claim 4: MacDoran teaches claim 3. MacDoran teaches (Continued on Supplemental Sheet.)

Supplemental Box

(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: Boxes I - VIII

Sheet 10

I. BASIS OF REPORT:

This report has been drawn on the basis of the description,
page(s) 1-4, 6-14, 17-18, as originally filed.
page(s) NONE, filed with the demand.
and additional amendments:
Pages 5, 15-16, filed with the letter of 19 April 2001.

This report has been drawn on the basis of the claims,
page(s) 19-23, 25-27, as originally filed.
page(s) NONE, as amended under Article 19.
page(s) NONE, filed with the demand.
and additional amendments:
Page 24, filed with the letter of 19 April 2001.

This report has been drawn on the basis of the drawings,
page(s) 1-3, as originally filed.
page(s) NONE, filed with the demand.
and additional amendments:
NONE

This report has been drawn on the basis of the sequence listing part of the description:
page(s) NONE, as originally filed.
pages(s) NONE, filed with the demand.
and additional amendments:
NONE

V. 2. REASONED STATEMENTS - CITATIONS AND EXPLANATIONS (Continued):

comprising the further step of forwarding the ODB and associated URH to the local distribution controller (col. 10, lines 34-48).

Claim 5: MacDoran teaches claim 3. MacDoran teaches the URH is forwarded to the main server, further comprising the steps of: communicating the ODB from the local distribution controller to the local distribution server (col. 10, lines 31-41).

Claim 6: MacDoran teaches claim 5. MacDoran teaches the ODB is processed at the local distribution controller to generate a second ODB, which second ODB is forwarded from the local distribution controller to the local distribution server (col. 29, lines 61-67 and col. 30, lines 1-11).

Claim 7: MacDoran teaches claim 3. MacDoran teaches the pre-encrypted content is broadcast (col. 10, lines 26-31), the ODB is broadcast (col. 10, lines 26-34), and only a user terminal with appropriate entitlement authorization will be able to decrypt the broadcast content (col. 10, lines 26-54).

Claim 9: MacDoran teaches claim 3. MacDoran teaches the pre-encrypted content is singlecast (col. 28, lines 26-31), the ODB is singlecast (col. 28, lines 26-44), and only a user terminal with appropriate entitlement authorization will be able to decrypt the singlecast content (col. 28, lines 39-44).

Claim 10: MacDoran teaches claim 3. MacDoran teaches the entitlement authorization comprises at least one of (i) an entitlement authorization for a service carrying the content, (ii) an entitlement authorization for the content itself, and (iii) an entitlement authorization for using ODB (col. 10, lines 26-54 or col. 12, lines 48-62).

Claim 11: MacDoran teaches claim 3. MacDoran teaches forwarding the ODB from a server application via an application program interface in the user terminal to a kernel located in the user terminal (col. 29, lines 8-15), processing the ODB in conjunction with the received entitlement authorization such that the processor determines whether to decrypt the received pre-encrypted content (col. 10, lines 26-54), receiving the pre-encrypted content (col. 10, lines 26-34), decrypting the pre-encrypted content when authorization is granted (col. 11, lines 31-48), and processing the decrypted content for display (col. 11, lines 31-48).

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/US00/09800

Supplemental Box

(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: Boxes I - VIII

Sheet 11

Claim 12: MacDoran teaches claim 11. MacDoran teaches the pre-encrypted content is received by the secure processor via direct memory access from device memory (col. 28, lines 53-67 and col. 29, lines 1-8).

Claim 13: MacDoran teaches claim 11. MacDoran teaches the pre-encrypted content is received by the secure processor via direct memory access from device memory (col. 28, lines 53-67 and col. 29, lines 1-18).

Claim 14: MacDoran teaches claim 3. MacDoran teaches the ODB is coded in a manner that is not readily discernable by third parties (col. 29, lines 37-44).

Claim 16: MacDoran teaches claim 3. MacDoran teaches ODB itself is encrypted (col. 29, lines 37-44).

Claim 18: MacDoran teaches claim 3. MacDoran teaches the user terminal is one of a set-top box, a digital television or a host with point-of-deployment capability, or a personal computer (col. 15, lines 40-47).

Claim 19: MacDoran teaches claim 3. MacDoran teaches one of the URH and the ODB is stored as an attribute of the pre-encrypted content (col. 17, lines 64-67 and col. 18, lines 1-12).

Claim 20: MacDoran teaches claim 3. MacDoran teaches each of the URH and the ODB are stored as an attribute of the pre-encrypted content (col. 17, lines 64-67 and col. 18, lines 1-12).

Claim 21: MacDoran teaches claim 3. MacDoran teaches the pre-encrypted content is accessed via the Internet (col. 13, lines 19-27).

Claims 8, 22-35, and 37-42 lack an inventive step under PCT Article 33(3) as being obvious over MacDoran in view of Mittra.

Claim 8: MacDoran teaches claim 3. Mittra teaches the pre-encrypted content is multicast (col. 2, lines 1-45), the ODB is multicast (col. 1, lines 59-67), and only a user terminal with appropriate entitlement authorization will be able to decrypt the multicast content (col. 1, lines 59-67 and col. 2, lines 58-67).

Claim 22: MacDoran teaches claim an apparatus for providing access control for pre-encrypted on-demand content (col. 28, lines 53-67), an encryption device for encrypting the content (col. 29, lines 1-18), a server for receiving the pre-encrypted content from the encryption device (col. 10, lines 26-34), a pre-encryption controller for generating a first tag and an associated second tag, the second tag acting as a reference to the pre-encrypted content and associated first tag, wherein the first tag and second tag are unique to the pre-encrypted content and are tracked by the pre-encryption controller (col. 10, lines 31-54), and a user terminal for receiving entitlement authorization associated with the pre-encrypted content (col. 13, lines 45-63), and the first tag being communicated to a user terminal and the second tag being communicated to the server (col. 13, lines 45-63). Mittra teaches the user terminal determines whether it is authorized to access the pre-encrypted content based on the entitlement authorization and the first tag upon demand of the content by a user (col. 13, lines 45-63).

Claim 23: MacDoran in view of Mittra teaches claim 22. MacDoran teaches the pre-encryption controller is in communication with a local distribution controller communicates the entitlement authorization to the user terminal (col. 14, lines 42-56). Mittra teaches the server is a main server (col. 7, lines 11-14) and the main server communicates the pre-encrypted content and first tag to the user terminal via local distribution server (col. 7, lines 11-14).

Claim 24: MacDoran in view of Mittra teaches claim 23. MacDoran teaches the first tag is an opaque data block (ODB) (col. 10, lines 31-54) and the second tag is a unique reference handle (URH) (col. 10, lines 48-54).

Claim 25: MacDoran in view of Mittra teaches claim 24. MacDoran teaches the local distribution controller receives the ODB and associated URH from the pre-encryption controller (col. 10, lines 26-54).

Claim 26: MacDoran in view of Mittra teaches claim 24. MacDoran teaches the main server receives only the URH from the pre-encryption controller (col. 10, lines 48-54) and the local distribution controller communicates the ODB to the local distribution server (col. 10, lines 31-54).

Claim 27: MacDoran in view of Mittra teaches claim 26. MacDoran teaches the ODB is processed at the local distribution controller to generate a second ODB, which second ODB is forwarded from the local distribution controller to the local

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/US00/09800

Supplemental Box

(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: Boxes I - VIII

Sheet 12

distribution server (col. 29, lines 61-67 and col. 30, lines 1-11).

Claim 28: MacDoran teaches the pre-encryption content is broadcast (col. 10, lines 26-31), the ODB is broadcast (col. 10, lines 26-34), and only a user terminal with appropriate entitlement authorization will be able to decrypt the broadcast content (col. 10, lines 26-54).

Claim 29: MacDoran in view of Mittra teaches claim 24. Mittra teaches the pre-encrypted content is multicast (col. 2, lines 1-45), the ODB is multicast (col. 1, lines 59-67), and only a user terminal with appropriate entitlement authorization will be able to decrypt the multicast content (col. 2, lines 58-67).

Claim 30: MacDoran in view of Mittra teaches claim 24. MacDoran teaches the pre-encrypted content is singlecast (col. 28, lines 20-31), the ODB is singlecast (col. 28, lines 26-44), and only a user terminal with appropriate entitlement authorization will be able to decrypt the singlecast content (col. 28, lines 39-44).

Claim 31: MacDoran in view of Mittra teaches claim 24. MacDoran teaches entitlement authorization comprises at least one of (i) an entitlement authorization for a service carrying the content, (ii) an entitlement authorization for the content itself, (iii) an entitlement authorization for using ODB (col. 10, lines 26-54 and col. 12, lines 48-62).

Claim 32: MacDoran in view of Mittra teaches claim 24. MacDoran teaches a client application using a program interface for forwarding the ODB from the local distribution server to a kernel (col. 28, lines 8-15), the kernel receiving the ODB the application program interface and the entitlement authorization from the local distribution controller (col. 29, lines 8-15), and a secure processor for receiving the ODB and entitlement authorization from the kernel and receiving the pre-encrypted content from the local distribution server (col. 29, lines 8-15), and the processor processes the ODB in conjunction with entitlement authorization such that the processor determines whether to decrypt the received pre-encrypted content (col. 10, lines 26-54).

Claim 33: MacDoran in view of Mittra teaches claim 24. MacDoran teaches the secure processor receives the pre-encrypted content via a receiver circuit (col. 10, lines 26-54).

Claim 34: MacDoran in view of Mittra teaches claim 24. MacDoran teaches the secure processor receives the pre-encrypted content via direct memory access from device memory (col. 28, lines 53-67 & col. 29, lines 1-18).

Claim 35: MacDoran in view of Mittra teaches claim 24. MacDoran teaches the ODB is coded in a manner that is not readily discernable by third parties (col. 29, lines 37-44).

Claim 37: MacDoran in view of Mittra teaches claim 24. Mittra teaches the ODB itself is encrypted (col. 8, lines 15-22).

Claim 38: MacDoran in view of Mittra teaches claim 37. Mittra teaches the ODB is encrypted using the user's public key (col. 8, lines 15-22).

Claim 39: MacDoran in view of Mittra teaches claim 24. Mittra teaches the user terminal is one of a set-top box, a digital television or a host with point-of-deployment capability (col. 4, lines 45-67).

Claim 40: MacDoran in view of Mittra teaches claim 24. MacDoran teaches one of the URH and the ODB is stored as an attribute of the pre-encrypted content (col. 17, lines 64-67 and col. 18, lines 1-12).

Claim 41: MacDoran in view of Mittra teaches claim 24. MacDoran teaches each of the URH and the ODB are stored as an attribute of the pre-encrypted content (col. 17, lines 64-67 and col. 18, lines 1-12).

Claim 42: MacDoran in view of Mittra teaches claim 24. MacDoran teaches the pre-encrypted content is accessed via the Internet (col. 13, lines 19-27).

Claims 15 and 17 lack an inventive step under PCT Article 33(3) as being obvious over MacDoran in view of Lidinsky.

Claim 15: MacDoran in view of Mittra teaches claim 3. Mittra teaches the ODB content includes one of an encryption key or a hierarchy of encryption keys (col. 46, lines 60-63).

Claim 17: MacDoran in view of Mittra teaches claim 16. MacDoran teaches the ODB is encrypted using the user's public

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/US00/09800

Supplemental Box

(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: Boxes I - VIII

Sheet 13

key (col. 46, lines 60-63).

Claim 36 lacks an inventive step under PCT Article 33(3) as being obvious over MacDoran in view of Mittra, further in view of Lidinsky.

Claim 36: MacDoran in view of Mittra teaches claim 24. Lidinsky teaches the ODB content includes one of an encryption key or a hierarchy of encryption keys (col. 46, lines 60-63).

----- NEW CITATIONS -----

US 5,748,736 A (MITTRA et al) 05 MAY 1998, see column 1-4 & 7-8, lines 1-67.

US 5,757,916 A (MACDORAN et al) 06 OCTOBER 1995, see column 10-15 & 28-30.

US 4,897,874 A (LIDINSKY et al) 03 MARCH 1988, see column 46, lines 60-63.

SUMMARY OF THE INVENTION

In accordance with the present invention, a method and apparatus are provided for access control of pre-encrypted on-demand content. In a simplified embodiment, the content is pre-encrypted by an encryption device controlled by a pre-encryption controller. The pre-encrypted content is forwarded from the encryption device to a server. The server may be a main server or a local distribution server. The pre-encryption controller provides a first tag to the user terminal and a second tag to the server. The first tag is associated with the second tag and the second tag acts as a reference to the pre-encrypted content and associated first tag, wherein said first and second tags are unique to the pre-encrypted content and are tracked by the pre-encryption controller. The pre-encrypted content is communicated from the server to a user terminal via a first communication path.

20 An entitlement authorization associated with the encrypted content is communicated to a user terminal (e.g., a "client device" such as a set-top box) via a second communication path independent of said first communication path. Authorization to

25 access the pre-encrypted content is determined based on said entitlement authorization and said first tag upon demand of said content by a user.

The user terminal may be a set-top box, a

security. In the on-demand case, the ODB itself may also be encrypted (with an additional level of implementation complexity) using, for example, the recipient's public key. In the case of broadcast or
5 multicast content, the ODB may be made available in advance since it is associated with the event or content to be viewed or received. Encryption of the ODB using the user's public key is extremely useful for the IP transport case where the system
10 administrator has the option to make known what events are available when, e.g. via an Electronic Programming Guide (EPG). In this manner the ODB content is securable as deemed necessary without burdening the content providers or service vendors.
15 In addition, the entitlement control is upgradeable without impacting the content providers or service vendors.

The pre-encrypted content may be broadcast, multicast, or singlecast such that only a user
20 terminal 20 with appropriate entitlement authorization will be able to decrypt the broadcast, multicast, or singlecast content. Alternatively, the pre-encrypted content may be accessed via the Internet.

25 The entitlement authorization may comprise at least one of (i) an entitlement authorization for a service carrying the content, (ii) an entitlement authorization for the content itself, and (iii) an entitlement authorization for using the ODB.

Figure 3 depicts the processing that takes place at the user terminal 20. The client application 40 (typically residing in a user terminal 20 such as a set-top box) requests specific content from the server (either the server 12 of Figure 1 or local distribution server 18 of Figure 2), such as a video on demand (VOD) movie or any other interactive content. The server then sends the ODB to the client application device 40. After this set-up is completed, the server 18 starts sending the pre-encrypted content to the user terminal 20.

The client application 40 (e.g. software) running in the user terminal processor (CPU) 36 receives the ODB from a server application in the server 12 or local distribution server 18, as described in connection with Figures 1 and 2, and forwards it via an application program interface (API) 42 to the user terminal processor kernel 44. In the broadcast and multicast modes, the ODB may be made available ahead of time, before the actual broadcast or multicast event commences. In this case the ODB may be requested by and sent to the user by the local distribution controller (16). The ODB is then processed in the user terminal 20 in conjunction with the received entitlement authorization (as described in connection with Figures 1 and 2) to determine whether to decrypt the received pre-encrypted content.

authorization associated with the pre-encrypted content;

said first tag being communicated to the user terminal and said second tag being communicated to the server;

wherein the user terminal determines whether it is authorized to access said pre-encrypted content based on said entitlement authorization and said first tag upon demand of said content by a user.

23. An apparatus in accordance with claim 22, wherein;

the server is a main server;

the main server communicates the pre-encrypted content and first tag to the user terminal via a local distribution server; and

the pre-encryption controller is in communication with a local distribution controller, which local distribution controller communicates the entitlement authorization to the user terminal.

24. An apparatus in accordance with claim 23, wherein:

the first tag is an opaque data block (ODB); and

the second tag is a unique reference handle (URH).

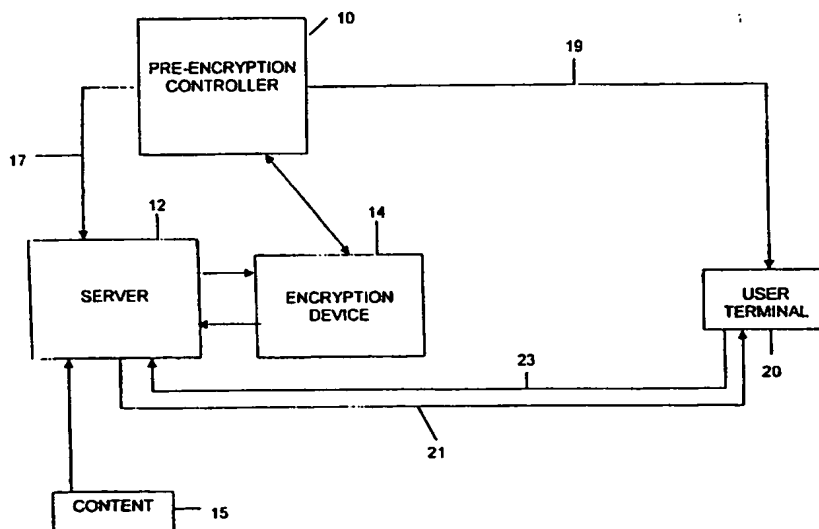
25. An apparatus in accordance with claim 24, wherein the local distribution controller receives the ODB and associated URH from the pre-encryption controller.



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁷ : H04N 7/16, 7/173		A1	(11) International Publication Number: WO 00/67483
			(43) International Publication Date: 9 November 2000 (09.11.00)
(21) International Application Number: PCT/US00/09800 (22) International Filing Date: 12 April 2000 (12.04.00) (30) Priority Data: 60/132,366 4 May 1999 (04.05.99) US (71) Applicant (for all designated States except US): GENERAL INSTRUMENT CORPORATION [US/US]; 101 Tournament Drive, Horsham, PA 19044 (US). (72) Inventors; and (75) Inventors/Applicants (for US only): SAFADI, Reem [US/US]; 429 Brown Briar Circle, Horsham, PA 19044 (US). VINCE, Lawrence, D. [US/US]; 114 Aileen Drive, Lansdale, PA 19446 (US). (74) Agent: LIPSITZ, Barry, R.; 755 Main Street, Building No. 8, Monroe, CT 06468 (US).		(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published With international search report.	

(54) Title: METHOD AND APPARATUS FOR ACCESS CONTROL OF PRE-ENCRYPTED ON-DEMAND TELEVISION SERVICES



(57) Abstract

A method and apparatus for providing access control of pre-encrypted on-demand television content. Existing encryption capability for cable television services or the like is extended to handle pre-encrypted content from a server (12) that is requested on demand by a viewer at a user terminal (20). Alternatively, the pre-encrypted content (provided, e.g. by an encryption device (14) can be broadcast or multicast from the server (12) to a group of viewers. The invention is upgradeable to facilitate implementations of entitlement control algorithms that vary in sophistication as the need dictates. Additionally, the method is extensible to enable access control of pre-encrypted content that is independent of the transport protocol used. Such protocols include, for example, MPEG-2 and Internet Protocol (IP) which may also utilize Public Key Cryptography.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Larvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

METHOD AND APPARATUS FOR ACCESS CONTROL OF
PRE-ENCRYPTED ON-DEMAND TELEVISION SERVICES

This application claims the benefit of U.S.
provisional patent application no.60/132,366 filed
5 May 4, 1999.

BACKGROUND OF THE INVENTION

The present invention relates to the
communication of information services over a
communication network, and more particularly to
10 providing access control for signals containing
audiovisual content and services, such as on-demand
television programming. In order to render
subscription programming services and the like
commercially viable, systems must be provided for
15 preventing non-paying individuals from obtaining the
services. Such "access control" systems can take
various forms, but generally include some type of
modification (e.g., scrambling) or encryption of the
signals that carry the services. Only authorized
20 subscribers have access to the elements (e.g.,
cryptographic keys) necessary to satisfactorily
receive the signals.

Current techniques for decryption of signals
such as on-demand services may be based on real time
25 hardware based encryption solutions or based on pre-
encryption methods. Some configurations allow for

cost effective real time encryption at the transport level but are not as effective at a service level.

Such problems, together with the following

additional factors, require a new solution that

5 provides a reliable and cost-effective means for access control of on-demand services:

1. Current real-time encryption does not meet the cost model for on-demand services, in that it is expensive to implement.
- 10 2. In some configurations real time encryption requires too much real-estate at service provider sites (currently, for example, various video-on-demand (VOD) vendors are consolidating their servers and signal
- 15 modulators (e.g., QAM modulators) in space efficient packaging which bypasses a real-time encryption stage).
3. Pre-encryption is inherently not as secure as real-time encryption. At the same time,
- 20 on-demand content security requirements are less stringent than those of broadcast content. For example, there is no *a priori* knowledge of when certain content will be requested in the on-demand case. In the
- 25 broadcast case, the content is always being sent and the schedules are known ahead of time.
4. MPAA (Motion Picture Association of America) has issues with clear (i.e., unencrypted)

content, such as movies, and expects such content to be protected.

- 5 5. Entitlement control should be upgradeable without impacting content providers or server vendors. Stronger solutions should be able to be incorporated gradually as the need dictates.
- 10 6. Secure content delivery of MPEG-2 (Motion Picture Experts Group) using Internet Protocol (IP) for point to point on demand services or multicast services must be facilitated.
7. Transport independent entitlement control (e.g., MPEG-2 or IP) must be provided.

15 It would be advantageous to provide a method and apparatus for access control of on-demand services that addresses the above-noted issues. In particular, it would be advantageous to provide a content pre-encryption method that enables
20 entitlement control to be effectively implemented independent of the transport protocol, e.g., MPEG-2 or IP.

 It would be still further advantageous to provide such a capability that can be offered as a
25 separate service to content providers, server vendors, and cable system operators. The present invention can be adapted for use with different

types of provider networks, e.g. satellite and Internet based networks.

The present invention provides a system having these and other advantages. In particular, the invention disclosed herein extends existing encryption capability, such as that provided by the Digicipher II (DCII) system available from General Instrument Corporation of Horsham, Pennsylvania, USA, the assignee of the present invention, to handle pre-encrypted content that is requested on demand by a viewer or is sent to a group of viewers. The method of the invention is also upgradeable to facilitate implementations of entitlement control algorithms that vary in sophistication as the need dictates. Additionally, the method is extensible to enable encryption control that is independent of the transport protocol used. Such protocols include, for example, MPEG-2 and Internet Protocol (IP).

SUMMARY OF THE INVENTION

In accordance with the present invention, a method and apparatus are provided for access control of pre-encrypted on-demand content. In a simplified embodiment, the content is pre-encrypted by an encryption device controlled by a pre-encryption controller. The pre-encrypted content is forwarded from the encryption device to a server. The server may be a main server or a local distribution server. The pre-encryption controller provides a first tag to the user terminal and a second tag to the server. Said first tag being associated with said second tag and said second tag acts as a reference to the pre-encrypted content and associated first tag, wherein said first and second tags are unique to the pre-encrypted content and are tracked by the pre-encryption controller. The pre-encrypted content is communicated from the server to a user terminal via a first communication path.

An entitlement authorization associated with the encrypted content is communicated to a user terminal (e.g., a "client device" such as a set-top box) via a second communication path independent of said first communication path. Authorization to access the pre-encrypted content is determined based on said entitlement authorization and said first tag upon demand of said content by a user.

The user terminal may be a set-top box, a

digital television or a host with point-of-deployment (POD) capability, or a personal computer (PC) or the like that provides the functionality of a set-top box.

5 The pre-encryption controller acts to set up the encryption device for pre-encrypting the content. The set up of the encryption device is outside the scope of this invention. For background purposes, it will suffice to state that the pre-
10 encryption controller, through bi-directional communication with the encryption device, configures the encryption device with appropriate parametric values and commands to enable the encryption device appropriately to encrypt the content.

15 In an alternate embodiment, the server is a main server (e.g., a head-end server) which communicates the pre-encrypted content and first tag to the user terminal via a local distribution server. The pre-encryption controller is in
20 communication with a local distribution controller (e.g., a head-end controller in a cable television implementation), which local distribution controller communicates the entitlement authorization to the user terminal.

25 In a preferred embodiment, the first tag is an opaque data block (ODB) and the second tag is a unique reference handle (URH). The URH may be generated as a function of the ODB.

 In one embodiment, the ODB and URH are both

forwarded to both the local distribution controller and the server from the pre-encryption controller.

In an alternate embodiment, only the URH is forwarded to the main server and the ODB is communicated from the local distribution controller to the local distribution server.

In one embodiment the ODB or the URH may be stored as an attribute of the encrypted content. Alternatively, both the URH and the ODB are stored as an attribute of the encrypted content.

The ODB may be processed at the local distribution controller to generate a second ODB, which second ODB is forwarded from the local distribution controller to the local distribution server. This processing at the local distribution controller may include algorithmically modifying the ODB. Such reprocessing of the ODB at the local distribution controller provides an added level of security since the post-processing ODBs are no longer the same across multiple local distribution controllers.

The ODB itself may be coded in a manner that is not readily discernable by third parties.

Alternatively, the ODB content may include an encryption key to be used for decryption or used to derive the key for decryption. The ODB may also include a hierarchy of encryption keys whose ultimate use is the derivation of the relevant key for decryption but with added levels of security. In

this manner the ODB content is securable as deemed necessary without burdening the content providers or service vendors. In the on-demand case, the ODB itself may also be encrypted, using, for example,
5 the recipient's public key.

The pre-encrypted content may be broadcast, multicast, or singlecast such that only a user terminal with appropriate entitlement authorization will be able to decrypt the broadcast, multicast, or
10 singlecast content. Alternatively, the pre-encrypted content may be accessed via the Internet.

The entitlement authorization may comprise at least one of (i) an entitlement authorization for a service carrying the content, (ii) an entitlement
15 authorization for the content itself, and (iii) an entitlement authorization for using ODB.

In a preferred embodiment, a client application (typically software residing in a user terminal such as a set-top box) then requests specific content
20 from the server, such as a video on demand (VOD) movie or any other interactive content. The ODB is forwarded from a server application to the client application software that typically resides in a central processor (CPU) of the user terminal. After
25 this set-up is completed, the server starts sending the pre-encrypted content to the user terminal. The ODB is then forwarded from the client application via an application program interface in the CPU to a kernel located in the user terminal. The ODB is then

processed in the user terminal in conjunction with the received entitlement authorization to determine whether to decrypt the received pre-encrypted content.

5 Processing may be provided by a secure processor located in the user terminal or a software task included in the user terminal CPU. The pre-encrypted content is received by the user terminal and decrypted when authorization is granted. Upon
10 authorization, the content will be processed for display.

 The pre-encrypted content may be received by the secure processor via a conventional receiver circuit. Alternatively, the pre-encrypted content
15 may be received by the secure processor via direct memory access from device memory.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of the functional components of the flexible pre-encryption architecture of the invention;

5 Figure 2 is a block diagram of another embodiment of the functional components of the flexible pre-encryption architecture of the invention; and

10 Figure 3 is a block diagram of the relevant components of a user terminal in accordance with the invention.

DETAILED DESCRIPTION OF THE INVENTION

Figure 1 illustrates the main components of an on-demand content communication system in accordance with the present invention. In particular, a method and apparatus are provided for access control of pre-encrypted on-demand content. The video encoder and post encoding processors are not shown, since they are well known in the art. As will be appreciated by those skilled in the art, any type of post processing to be done on the content file/data stream is performed prior to encryption.

Referring to Figure 1, a pre-encryption controller 10 sets up an encryption device 14 for encryption of the content 15. A server 12 forwards the content file/stream to the encryption device 14 for encryption of the content prior to distribution ("pre-encryption"). The encryption device encrypts the content file and forwards the pre-encrypted content back to the main server 12.

The pre-encryption controller 10 acts to set up the encryption device 14 for pre-encrypting the content. The set up of the encryption device 14 is outside the scope of this invention. For background purposes, it will suffice to state that the pre-encryption controller 10, through bi-directional communication with the encryption device 14, configures the encryption device 14 with appropriate parametric values and commands to enable the

encryption device 14 appropriately to encrypt the content.

In one embodiment as shown in Figure 1, the pre-encrypted content is forwarded from the encryption device 14 to a server 12. The server may be a main server or a local distribution server. The pre-encryption controller provides a first tag and a second tag to the server 12 via line 17. The first tag is also provided to a user terminal 20 via line 19 or 21 depending upon the particular implementation, the first tag being associated with said second tag. The second tag acts as a reference to the pre-encrypted content and associated first tag, wherein the first and second tags are unique to the pre-encrypted content and are tracked by the pre-encryption controller 10. The pre-encrypted content is communicated from the server 12 to a user terminal 20 (e.g., a "client device" such as a set-top box) via a first communication path 21.

An entitlement authorization associated with the encrypted content is communicated to the user terminal 20 via a second communication path 19 independent of the first communication path. Authorization to access the pre-encrypted content is determined at the user terminal 20 based on said entitlement authorization and the first tag upon demand of the content by a user. Communication from the user terminal 20 back to the server 12 is provided on line 23.

The user terminal 20 may be a set-top box, a digital television or a host with point-of-deployment (POD) capability, or a personal computer (PC) or the like that provides the functionality of a set-top box.

In an alternate embodiment shown in Figure 2, the server is a main server 12' (e.g., a head-end server) which communicates the pre-encrypted content and first tag to the user terminal 20 via lines 25 and 27 and a local distribution server 18. The main server 12' can distribute the encrypted content to various local distribution servers (at various service provider locations, e.g., head-ends). The pre-encryption controller 10 is in communication with a local distribution controller 16, which controls, e.g., a cable television system or the like in a well known manner (e.g., a head-end controller in a cable television implementation). The local distribution controller 16 communicates the entitlement authorization to the user terminal 20 via line 29.

In a preferred embodiment, the first tag is an opaque data block (ODB) and the second tag is a unique reference handle (URH). The URH may be generated as a function of the ODB.

In one embodiment, the ODB and URH are both forwarded to both the local distribution controller 16 (via line 11) and the main server 12' (via line 13) from the pre-encryption controller 10. In an

alternate embodiment, only the URH is forwarded to the main server 12' and the ODB is communicated from the local distribution controller 16 to the local distribution server 18 via line 22.

5 Either the ODB or the URH may be stored as an attribute of the encrypted content. Alternatively, both the URH and the ODB may be stored as an attribute of the encrypted content.

 The ODB may be processed at the local
10 distribution controller 16 to generate a modified, second ODB, which second ODB is forwarded from the local distribution controller 16 to the local distribution server 18. This processing at the local distribution controller 16 may include
15 algorithmically modifying the ODB. This may be done as an offline process. Such reprocessing of the ODB at the local distribution controller 16 provides an added level of security since the post-processing ODBs are no longer the same across multiple local
20 distribution controllers.

 The system manufacturer specifies the ODB content and, for security reasons, the ODB itself may be coded in a manner that is not readily discernable by third parties. Alternatively, the ODB
25 content may include an encryption key to be used for decryption or used to derive the key for decryption. The ODB may also include a hierarchy of encryption keys whose ultimate use is the derivation of the relevant key for decryption but with added levels of

security. In the on-demand case, the ODB itself may also be encrypted (with an additional level of implementation complexity) using, for example, the recipient's public key. In the case of broadcast or
5 multicast content, the ODB may be made available in advance since it is associated with the event or content to be viewed or received. Encryption of the ODB using the user's public key is extremely useful for the IP transport case where the system
10 administrator has to the option to make known what events are available when, e.g. via an Electronic Programming Guide (EPG). In this manner the ODB content is securable as deemed necessary without burdening the content providers or service vendors.
15 In addition, the entitlement control is upgradeable without impacting the content providers or service vendors.

The pre-encrypted content may be broadcast, multicast, or singlecast such that only a user
20 terminal 20 with appropriate entitlement authorization will be able to decrypt the broadcast, multicast, or singlecast content. Alternatively, the pre-encrypted content may be accessed via the Internet.

25 The entitlement authorization may comprise at least one of (i) an entitlement authorization for a service carrying the content, (ii) an entitlement authorization for the content itself, and (iii) an entitlement authorization for using ODB.

Figure 3 depicts the processing that takes place at the user terminal 20. The client application 40 (typically residing in a user terminal 20 such as a set-top box) then requests
5 specific content from the server (either the server 12 of Figure 1 or local distribution server 18 of Figure 2), such as a video on demand (VOD) movie or any other interactive content. The server then sends the ODB to the client application device 40. After
10 this set-up is completed, the server 18 starts sending the pre-encrypted content to the user terminal 20.

The client application 40 (e.g. software) running in the user terminal processor (CPU) 36
15 receives the ODB from a server application in the server 12 or local distribution server 18, as described in connection with Figures 1 and 2, and forwards it via an application program interface (API) 42 to the user terminal processor kernel 44.
20 In the broadcast and multicast modes, the ODB may be made available ahead of time, before the actual broadcast or multicast event commences. In this case the ODB may be requested by and sent to the user by the local distribution controller (16). The
25 ODB is then processed in the user terminal 20 in conjunction with the received entitlement authorization (as described in connection with Figures 1 and 2) to determine whether to decrypt the received pre-encrypted content.

Processing may be provided by a secure processor 32 located in the user terminal 20 or a software task included in the CPU 36. The pre-encrypted content is received by the user terminal
5 20 and decrypted when authorization is granted. Upon authorization, the content will be processed for display.

The pre-encrypted content may be received by the secure processor 32 via a conventional receiver
10 circuit (i.e. receiver output of Figure 3). Alternatively, the pre-encrypted content may be received by the secure processor 32 via direct memory access from device memory 30. The decrypted output from the secure processor 32 is written back
15 to memory 30 for further use by the CPU 36, or is forwarded to a demultiplexer/decoder 34 for further processing in a conventional manner.

It should now be appreciated that the present invention provides an improved method and apparatus
20 for the delivery and access of pre-encrypted on-demand television services. In particular, the present invention provides a content pre-encryption method and apparatus that enables entitlement control to be effectively implemented independent of
25 the transport protocol, e.g., MPEG-2 or Internet Protocol (IP), and to some extent independent of transmission mode (i.e., singlecast (e.g., on-demand), multicast, or broadcast). Additionally, the present invention provides encryption and access

control capability that can be offered as a separate service to content providers, server vendors, cable system operators, and/or Internet service providers, or the like. The present invention enables
5 entitlement authorization that can vary in sophistication as deemed necessary without burdening the content providers or service vendors. In addition, the entitlement control is upgradeable without impacting the content providers or service
10 vendors.

Although the invention has been described in connection with certain preferred embodiments, it should be appreciated that numerous adaptations and modifications may be made thereto without departing
15 from the scope of the invention as set forth in the claims.

What is claimed is:

1. A method of providing access control for pre-encrypted on-demand content, comprising the steps of:

pre-encrypting the content;

forwarding the pre-encrypted content to a server;

providing a first tag to a user terminal, said first tag being associated with a second tag;

said second tag acting as a reference to the pre-encrypted content and associated first tag, wherein said first and second tags are unique to the pre-encrypted content and are tracked by a pre-encryption controller;

providing at least said second tag to said server;

communicating the pre-encrypted content from said server to said user terminal via a first communication path;

communicating an entitlement authorization associated with the pre-encrypted content to said user terminal via a second communication path independent of said first communication path; and

determining whether said user terminal is authorized to access said pre-encrypted content based on said entitlement authorization and said first tag upon demand of said content by a user.

2. A method in accordance with claim 1, wherein;

the server is a main server;

the main server communicates the pre-encrypted content and first tag to the user terminal via a local distribution server; and

the pre-encryption controller is in communication with a local distribution controller, which local distribution controller communicates the entitlement authorization to the user terminal.

3. A method in accordance with claim 2, wherein:

the first tag is an opaque data block (ODB); and

the second tag is a unique reference handle (URH).

4. A method in accordance with claim 3, comprising the further step of forwarding the ODB and associated URH to the local distribution controller.

5. A method in accordance with claim 3, wherein only the URH is forwarded to the main server, further comprising the steps of:

communicating the ODB from the local distribution controller to the local distribution server.

6. A method in accordance with claim 5, wherein the ODB is processed at the local distribution controller to generate a second ODB, which second

ODB is forwarded from the local distribution controller to the local distribution server.

7. A method in accordance with claim 3, wherein;

the pre-encrypted content is broadcast;

the ODB is broadcast; and

only a user terminal with appropriate entitlement authorization will be able to decrypt the broadcast content.

8. A method in accordance with claim 3, wherein:

the pre-encrypted content is multicast;

the ODB is multicast; and

only a user terminal with appropriate entitlement authorization will be able to decrypt the multicast content.

9. A method in accordance with claim 3, wherein:

the pre-encrypted content is singlecast;

the ODB is singlecast; and

only a user terminal with appropriate entitlement authorization will be able to decrypt the singlecast content.

10. A method in accordance with claim 3, wherein the entitlement authorization comprises at least one of (i) an entitlement authorization for a service carrying the content, (ii) an entitlement authorization for the content itself, and (iii) an entitlement authorization for using ODB.

11. A method in accordance with claim 3, further comprising the steps of:

forwarding the ODB from a server application via an application program interface in the user terminal to a kernel located in the user terminal;

processing the ODB in conjunction with the received entitlement authorization such that the processor determines whether to decrypt the received pre-encrypted content;

receiving the pre-encrypted content;

decrypting the pre-encrypted content when authorization is granted; and

processing the decrypted content for display.

12. A method in accordance with claim 11, wherein the pre-encrypted content is received by the secure processor via a receiver circuit.

13. A method in accordance with claim 11, wherein the pre-encrypted content is received by the secure processor via direct memory access from device memory.

14. A method in accordance with claim 3, wherein the ODB is coded in a manner that is not readily discernable by third parties.

15. A method in accordance with claim 3, wherein the ODB content includes one of an encryption key or a hierarchy of encryption keys.

16. A method in accordance with claim 3, wherein the ODB itself is encrypted.

17. A method in accordance with claim 16,

wherein the ODB is encrypted using the user's public key.

18. A method in accordance with claim 3, wherein the user terminal is one of a set-top box, a digital television or a host with point-of-deployment capability, or a personal computer.

19. A method in accordance with claim 3, wherein one of the URH and the ODB is stored as an attribute of the pre-encrypted content.

20. A method in accordance with claim 3, wherein each of the URH and the ODB are stored as an attribute of the pre-encrypted content.

21. A method in accordance with claim 3, wherein the pre-encrypted content is accessed via the Internet.

22. An apparatus for providing access control for pre-encrypted on-demand content, comprising:

an encryption device for encrypting the content;

a server for receiving the pre-encrypted content from the encryption device;

a pre-encryption controller for generating a first tag and an associated second tag, said second tag acting as a reference to the pre-encrypted content and associated first tag, wherein said first tag and second tag are unique to the pre-encrypted content and are tracked by the pre-encryption controller;

a user terminal for receiving entitlement

authorization associated with the pre-encrypted content;

said first tag being communicated to a user terminal and said second tag being communicated to the server;

wherein the user terminal determines whether it is authorized to access said pre-encrypted content based on said entitlement authorization and said first tag upon demand of said content by a user.

23. An apparatus in accordance with claim 22, wherein;

the server is a main server;

the main server communicates the pre-encrypted content and first tag to the user terminal via a local distribution server; and

the pre-encryption controller is in communication with a local distribution controller, which local distribution controller communicates the entitlement authorization to the user terminal.

24. An apparatus in accordance with claim 23, wherein:

the first tag is an opaque data block (ODB);
and

the second tag is a unique reference handle (URH).

25. An apparatus in accordance with claim 24, wherein the local distribution controller receives the ODB and associated URH from the pre-encryption controller.

26. An apparatus in accordance with claim 24, wherein:

the main server receives only the URH from the pre-encryption controller; and

the local distribution controller communicates the ODB to the local distribution server.

27. An apparatus in accordance with claim 26, wherein the ODB is processed at the local distribution controller to generate a second ODB, which second ODB is forwarded from the local distribution controller to the local distribution server.

28. An apparatus in accordance with claim 24, wherein;

the pre-encrypted content is broadcast;

the ODB is broadcast; and

only a user terminal with appropriate entitlement authorization will be able to decrypt the broadcast content.

29. An apparatus in accordance with claim 24, wherein:

the pre-encrypted content is multicast;

the ODB is multicast; and

only a user terminal with appropriate entitlement authorization will be able to decrypt the multicast content.

30. An apparatus in accordance with claim 24, wherein:

the pre-encrypted content is singlecast;

the ODB is singlecast; and
only a user terminal with appropriate entitlement authorization will be able to decrypt the singlecast content.

31. An apparatus in accordance with claim 24, wherein the entitlement authorization comprises at least one of (i) an entitlement authorization for a service carrying the content, (ii) an entitlement authorization for the content itself, and (iii) an entitlement authorization for using ODB.

32. An apparatus in accordance with claim 24, wherein the user terminal comprises:

a client application using a program interface for forwarding the ODB from the local distribution server to a kernel

said kernel receiving the ODB the application program interface and the entitlement authorization from the local distribution controller; and

a secure processor for receiving the ODB and entitlement authorization from the kernel and receiving the pre-encrypted content from the local distribution server, wherein the processor processes the ODB in conjunction with entitlement authorization such that the processor determines whether to decrypt the received pre-encrypted content.

33. An apparatus in accordance with claim 32, wherein the secure processor receives the pre-encrypted content via a receiver circuit.

34. An apparatus in accordance with claim 32, wherein the secure processor receives the pre-encrypted content via direct memory access from device memory.

35. An apparatus in accordance with claim 24, wherein the ODB is coded in a manner that is not readily discernable by third parties.

36. An apparatus in accordance with claim 24, wherein the ODB content includes one of an encryption key or a hierarchy of encryption keys.

37. An apparatus in accordance with claim 24, wherein the ODB itself is encrypted.

38. An apparatus in accordance with claim 37, wherein the ODB is encrypted using the user's public key.

39. An apparatus in accordance with claim 24, wherein the user terminal is one of a set-top box, a digital television or a host with point-of-deployment capability, or a personal computer.

40. An apparatus in accordance with claim 24, wherein one of the URH and the ODB is stored as an attribute of the pre-encrypted content.

41. An apparatus in accordance with claim 24, wherein each of the URH and the ODB are stored as an attribute of the pre-encrypted content.

42. An apparatus in accordance with claim 24, wherein the pre-encrypted content is accessed via the Internet.

1/3

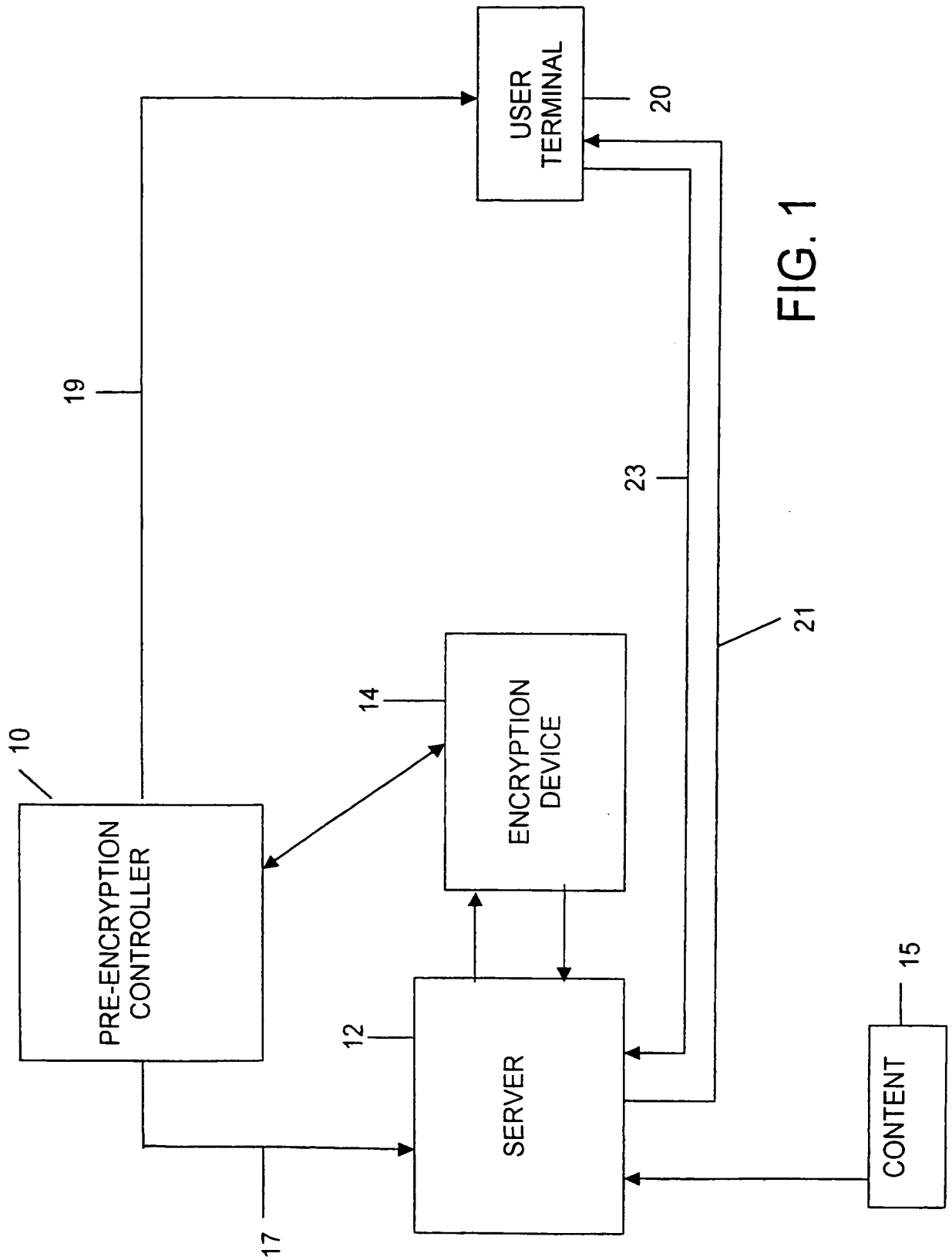
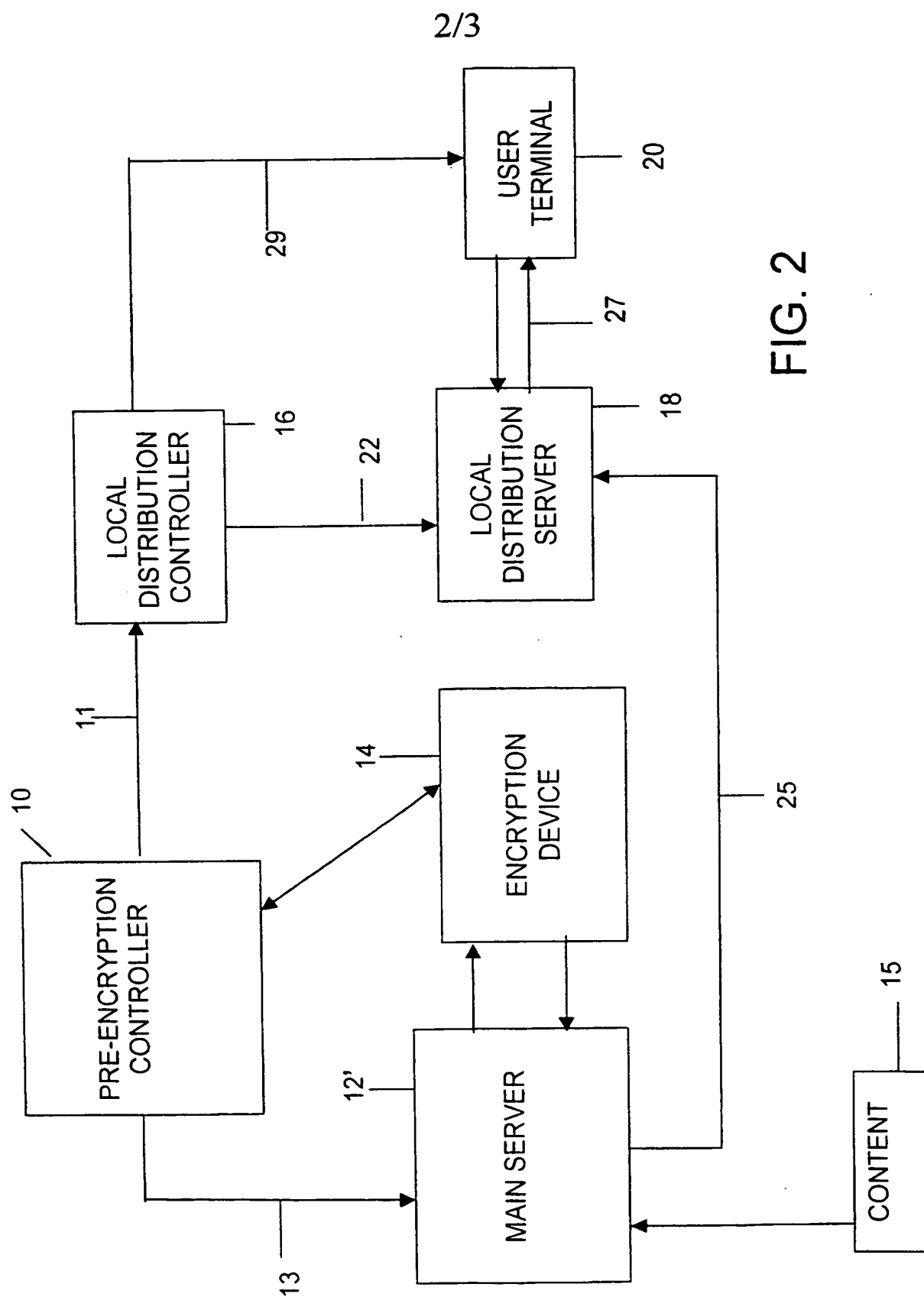


FIG. 1



3/3

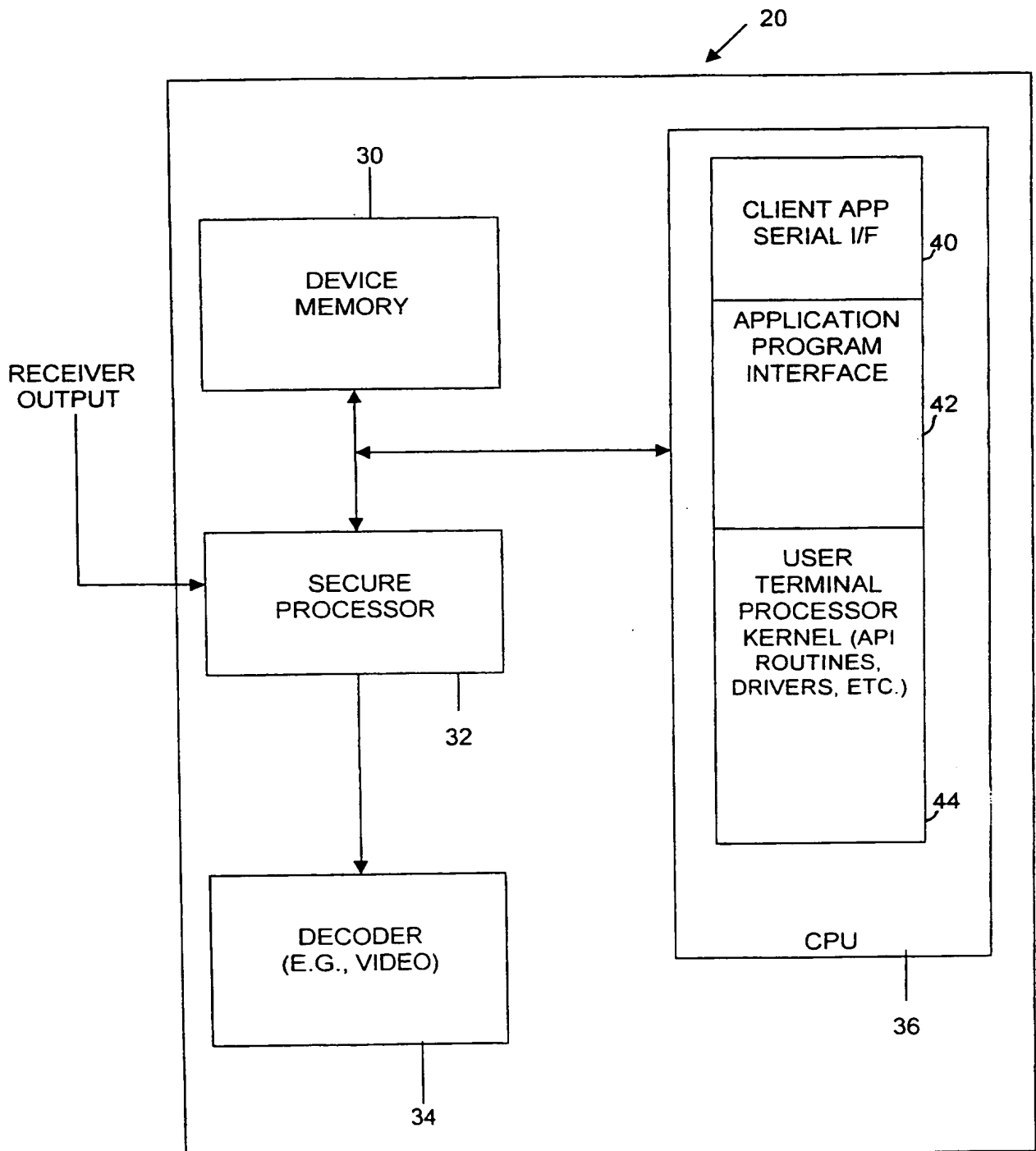


FIG. 3

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference GIC-574 PCT	FOR FURTHER ACTION see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/US 00/ 09800	International filing date (day/month/year) 12/04/2000	(Earliest) Priority Date (day/month/year) 04/05/1999
Applicant GENERAL INSTRUMENT CORPORATION et al.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 2 sheets.



It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

- a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.



the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

- b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :



contained in the international application in written form.



filed together with the international application in computer readable form.



furnished subsequently to this Authority in written form.



furnished subsequently to this Authority in computer readable form.



the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.



the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. ☐ **Certain claims were found unsearchable** (See Box I).

3. ☐ **Unity of invention is lacking** (see Box II).

4. With regard to the **title**,

the text is approved as submitted by the applicant.



the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

the text is approved as submitted by the applicant.



the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No.



as suggested by the applicant.



because the applicant failed to suggest a figure.



because this figure better characterizes the invention.

1



None of the figures.

INTERNATIONAL SEARCH REPORT

I. national Application No

PCT/US 00/09800

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04N7/16 H04N7/173

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 43426 A (TULLAYE PIERRE DE ;CANAL PLUS SA (FR); BAYASSI MULHAM (FR); JEZEQU) 1 October 1998 (1998-10-01) page 10, line 14 -page 16, line 19 page 19, line 18 -page 20, line 10 ---	1-4, 7-18, 22-25, 28-39
A	EP 0 793 366 A (HITACHI LTD) 3 September 1997 (1997-09-03) page 3, column 3, line 55 -column 4, line 42 page 5, column 7, line 55 -column 8, line 50 ---	1,2,22, 23
A	WO 99 14953 A (WORLDGATE COMMUNICATIONS INC) 25 March 1999 (1999-03-25) page 3, line 7 -page 4, line 4 -----	21,42

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

14 July 2000

Date of mailing of the international search report

20/07/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Van der Zaal, R

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 00/09800

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9843426	A	01-10-1998	AU 2770497 A	20-10-1998
			EP 0974229 A	26-01-2000
			NO 994532 A	19-11-1999
			PL 335585 A	08-05-2000
			AU 2770697 A	20-10-1998
			AU 7038198 A	20-10-1998
			WO 9843425 A	01-10-1998
			WO 9843162 A	01-10-1998
			WO 9843431 A	01-10-1998
			WO 9843248 A	01-10-1998
			WO 9843165 A	01-10-1998
			WO 9843415 A	01-10-1998
			WO 9843172 A	01-10-1998
			WO 9843433 A	01-10-1998
			WO 9843427 A	01-10-1998
			WO 9843437 A	01-10-1998
			WO 9843167 A	01-10-1998
			WO 9843428 A	01-10-1998
			WO 9843421 A	01-10-1998
			EP 0872798 A	21-10-1998
			EP 0866611 A	23-09-1998
			EP 0866616 A	23-09-1998
			EP 0866613 A	23-09-1998
			EP 0968610 A	05-01-2000
			EP 0968609 A	05-01-2000
			EP 0968607 A	05-01-2000
			EP 0974230 A	26-01-2000
			EP 0968468 A	05-01-2000
			EP 0968465 A	05-01-2000
			EP 0968602 A	05-01-2000
			EP 0968611 A	05-01-2000
			EP 0968608 A	05-01-2000
			EP 1010068 A	21-06-2000
			EP 1010331 A	21-06-2000
			EP 0968469 A	05-01-2000
			EP 1010320 A	21-06-2000
			EP 0972406 A	19-01-2000
			NO 994529 A	19-11-1999
			NO 994530 A	19-11-1999
			NO 994531 A	19-11-1999
			NO 994533 A	22-11-1999
			NO 994534 A	22-11-1999
			NO 994535 A	22-11-1999
			NO 994536 A	22-11-1999
			NO 994537 A	22-11-1999
			NO 994538 A	22-11-1999
			NO 994539 A	22-11-1999
			NO 994540 A	22-11-1999
			NO 994541 A	22-11-1999
EP 0793366	A	03-09-1997	JP 9230786 A	05-09-1997
			AU 693733 B	02-07-1998
			AU 1495297 A	18-09-1997
			AU 716807 B	09-03-2000
			AU 8786998 A	26-11-1998
			CN 1171682 A	28-01-1998
WO 9914953	A	25-03-1999	US 6049539 A	11-04-2000

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 00/09800

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9914953 A		AU 9378398 A NO 20001331 A	05-04-1999 05-05-2000
<hr/>			